THE DIR CYBERSECURITY INSIGHT

March FY2016 | DIR OCISO | DIRSECURITY@DIR.TEXAS.GOV

Privacy vs. Security

Newsfeeds have been saturated with stories concerning the Apple/FBI privacy controversy in recent days. In case you missed it, here's a summary of the issue: the FBI would like Apple to create custom firmware (calling it a backdoor) that would 1) bypass the number of times a passcode could be entered before the auto-wipe feature kicks in and 2) remove the delay time in-between password entry attempts. This would allow the investigators to unlock the iPhone of one of the San Bernardino shooters. Apple is fighting this injunction – explaining that this will set a dangerous precedent that makes all their customers' data inherently less secure.

This latest battle could have several implications for the security community and national security. In this situation we are forced to analyze the cost-benefit of privacy and information security versus national security.

On one side of this argument, security professionals have a responsibility to protect critical data. If government entities require companies and manufacturers to create products that are inherently less secure, the information security community must rapidly find ways to ensure newly exposed vulnerabilities are remediated and data remains protected. This also has tremendous implications on the future of policies and technology design decisions regarding digital privacy.

On the other side, the FBI has a responsibility of protecting the nation. If Apple does comply with the order, they could potentially give the FBI the capability to prevent attacks from occurring in the future. If Apple does not comply, we run the risk of preventing potential future attacks from occurring witch could carry its own consequences.

The battle raging on between Apple and the FBI forces the security community to consider the possible results of this issue and prepare for the worst case situation considering potentially vulnerable systems. Are security and privacy in a constant struggle against each other or are they allies? What do we have to compromise to achieve the best balance for our organization? As this clash continues, these are questions we as security professionals can examine to ensure we are prepared – regardless of the outcome of this case.

CONTENTS

Network Security Operations Center (NSOC)

Complimentary DIR Shred Day at ISF

Thursday, April 14

8:00 a.m. – 4:00 p.m.

Palmer Events Center

900 Barton Springs Road Austin, TX 78704

Are you attending ISF 2016? Bring your obsolete IT hardware with sensitive data and watch it be destroyed by EPC, CSI Leasing's wholly-owned subsidiary!

All agencies, schools, cities and counties are invited to bring up to 20 devices to be shredded on site at no charge. Devices can include hard drives, tapes, SSDs, cell phones, CDs and DVDs.

Receive a video of the process and access to Certificates of Data Destruction online.

Need to shred more than 20 devices? Please schedule an appointment with Patrick Mann at patrick.mann@epcusa.com

CSI LEASING
the power of experience

epc
Secure IT Asset Recovery
resell - recycle - relax

Archer Updates

DIR recently rolled out the Security Plan Template and Policy modules in Archer. To learn more about the new features available to you, please review the recorded web training.

Last session's appropriation bill, HB 1 Article IX, Section 10, requires DIR to submit a prioritization of state agencies' cybersecurity projects and projects to modernize or replace legacy systems, as defined in the October 2014 Legacy Systems Study, to be considered for funding to the Legislative Budget Board by Oct. 1, 2016. In order to be included in this prioritization, agencies must submit information about their requests to the department through the Archer online application. You can find additional information including a webinar recording that presented this function on the DIR resources web page.

Additionally, we will be adding functionality in the Risk Assessment process in Archer. These changes should be in effect by March 7. Please see significant changes below:

1. Addition of reports and dashboard views for a better user experience.
2. Ability to add a division to the Risk Assessable Unit (RAU) as well as applications, networks and locations. You can have the ability to assess your organization at a lower level. If you are interested in this capability, please contact grc@dir.texas.gov. This does not affect any current processes.
3. An RAU has to be saved first with required fields filled out before you are able to scope your RAU. You will be guided with reminders when a record is created.
4. At an assessment level, the user who creates the record will be defaulted as the reviewer in the security office field but it can be changed to someone within the security office.

Information Security Officer Spotlight

Samir J. Ghorayeb
Information Security Officer
Lamar State College – Port Arthur

I was born in Palestine and raised in Kuwait until I was 18 when I came to the United States to attend college. I am married and a father of three. My entire career has been in higher education beginning in 1989. I have worked at Volunteer State Community College as an ERP HR system programmer, then at Nashville State Technical Institute as a programmer also learning operating systems. I then moved to Tennessee State University as an Assistant Director for Information systems, and am now at Lamar State College – Port Arthur. I dabbled with just about everything including systems administration for Windows, VMS, and UNIX. I currently hold the titles of Director, CIO, IRM, and ISO.

Tell us how information security has changed since you started in your role.

Wow, imagine the late 80s, hardly any issues or exposure to the outside world existed. The concept at the time was just to make sure you have a username and a password. Now it would require a few books to explain what needs to be done. More than half of my time is spent on security and it takes my whole team to maintain that security.

What do you like best of your job?

Providing service on a global scale and seeing it through and getting the gratification of the accomplishments. Also dealing with some wonderful people while doing it.

What has been the greatest challenge that you have faced, and how did you resolved it?

Professionally, Hurricane Rita. Simply put, we were fully prepared but not quite prepared enough to continue to do business. The plans we had before Rita were rudimentary. Knowing what was critical and necessary to continue business in case of a disaster saved us from a lot of pain. It was baptism by fire, but we got through it with a bit of foresight, planning, and luck.

Tell us about your proudest accomplishment.

It was a project that introduced a campus-wide portal that included email (which students didn't have) with single sign-on to ERP and web-based systems in 2003. I believe we were one of the first colleges to do so at the time in Texas.

Top 3 life highlights.

Coming to America

Children, of course

Leading the effort to bring LSCPA to the next century technologically.

People would be surprised to know that you…

Watch Hallmark movies. ☺

If you were to write a book about yourself, what would you name it?

The trials and tribulations of a Palestinian Refugee…

What is the best advice you have received and that you have used?

Treat all as you like to be treated.

What would be your advice for a new security professional?

Read, read and then read again. Be vigilant, persistent and reach out to colleagues, internal auditors, DIR and any other resource possible.

OCISO Corner – Getting to Know the Team

Nancy Rainosek
Governance Risk and Compliance Program Manager
Department of Information Recourses

What is your responsibility in DIR and with the State?

I am the Governance Risk and Compliance Program Manager. I am responsible for the Archer system and bringing solutions for information security offices to use to enhance their security programs.

When and where did you start your career?

I began my career immediately after college as a methods analyst for Systems Division of the State Auditor's Office. The Systems Division provided systems development services, procurement reviews, and EDP reviews at state agencies and institutions of higher education.

Why the security field?

As a state government we have a responsibility to the citizens to secure their data. That's an important calling and an important role in ensuring government trust is maintained.

What is your personal back ground?

I was born in Cincinnati. We moved to Texas the summer before my senior year in high school. I always thought I would go back to Ohio but fate had different plans for me.

What did you think you were going to be when you grew up?

A teacher.

What is the greatest lesson you have learned?

Expect acceptance and show acceptance. I heard Debra Benton speak at a conference many years ago. Chapter two in her book, Executive Charisma, is called "Expect and Give Acceptance to Maintain Esteem." She says…

> *"As a human being walking this earth you have a right by birth to expect acceptance from everyone; and you have an obligation to give it to everyone. You can't expect it for yourself and not give it to others… If you don't expect acceptance, you won't get any".*

In other words, you should treat everyone equally, from the head of your organization to the lowest level employee. It takes a team to make an organization successful and it takes everyone to achieve the goals of the organization. That is best done by having respect for all positions and valuing their input and opinions.

What do you want your legacy to be?

I like to leave every place a little better than when I came. That's my goal.

Do you have a favorite hobby or pastime?

I show dogs. I have Shetland Sheepdogs. I've been on a break due to an extensive home remodeling project that has taken over my life for the past year and half. I'm looking forward to getting back into the dog show ring soon.

What do you like best about working at DIR?

The people. There are a lot of great people here dedicated to providing our customers with excellent services, who value each other's input and who contribute to a positive workplace

Insight from our Texas CISO

Eddie Block
CISO, State of Texas

"I'm from Windows and I'm here to help…"

Many of us have received a phone call claiming to be from Microsoft support warning of a virus identified on our computers. The caller walks you through verifying some files are on your computer and announces that yes, in fact, you do have a virus. The caller then offers to clean your PC for free, if you give them remote access. Of course, this is just a scam. The caller really wants access to your system to install malware and steal your personal information. I know it, you know it, but do your friends and family?

As tax season rounds the corner, many of us will get similar calls from "IRS representatives." The caller will try the scare tactics of jail, earnings garnishment, etc. Again, these calls are scams trying to convince the victim to give them a credit card number or wire funds.

While all of these scams are criminal, there is one that is particularly despicable, the "Grandmother Scam."[1] In this phone scam, the criminal calls elderly people as the grandchild of the victim. Usually the caller states that they have been arrested for DUI, are in prison and need bail money. Because the arrest is for DUI, the "grandchild" is really embarrassed and asks the grandparent to keep this between themselves.

This particular scam is so disgusting because it is preying on the elderly and their compassion for family.

I sit in my office with the titles of Chief Information Security Officer and Cybersecurity Coordinator for the great state of Texas. What technologies can I put into place to protect the elderly of Texas from these predatory con-men and women? Nix. Nada. Nothing.

The only thing that will really protect our citizens from this type of crime is awareness. That's where we, the security community, have to educate the larger community. Several groups, including the Consumer Federation of America[2], have published helpful information on this scam. However, it is also our responsibility to be champions for this type of information for our friends, families, churches, youth groups, and neighborhoods.

I know we are busy people, putting out fires, justifying budgets and trying to figure out how to secure the latest, greatest, shiny object to enter the network; few of us need another assignment. It is important, though, that we take the time to talk about security, online or over the phone, with those around us.

Eddie Block
CISO, State of Texas

---

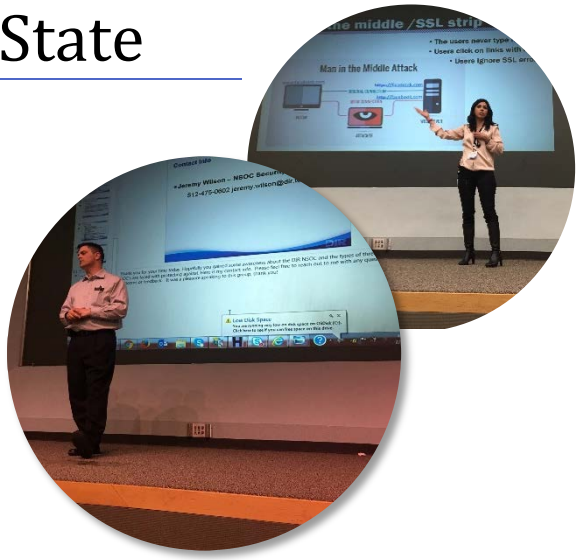
[1] https://www.washingtonpost.com/news/morning-mix/wp/2015/11/04/canadian-man-to-be-arraigned-in-florida-for-elaborate-multimillion-dollar-grandmother-scam/
[2] http://www.consumerfed.org/pdfs/Grandparent-Scam-Tips.pdf

Events

2015 Save the Dates

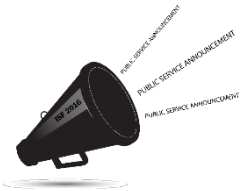
- Senate Business and Commerce Committee public hearing: March 30
- TASSCC Technology Education Conference: April 11
- Information Security Forum: April 14-15
- CyberTexas Conference: April 20-21

OCISO Participation Around the State



- Eddie Block attended the Information Sharing and Analysis Organization public meeting held February 9.
- Eddie Block participated on the State Agency Coordinating Committee Legal Affairs Subcommittee on February 12.
- Eddie Block, Claudia Escobar, Jeremy Wilson and Victor Westbrook presented "Understanding Cybersecurity: Attack Methods and Defenses" at the Executive Leadership for Information Technology Excellence (ELITE) program on February 17.
- Eddie Block attended the House of Urban Affairs Cybersecurity Hearing held February 23

ISF Public Service Announcement Challenge



The contest is open to agencies and higher institutes of education in Texas. To enter, submit a 30-second television public service announcement (PSA) that highlights one Information Security Awareness topic.

Submissions will be evaluated based on originality of messaging, pacing and overall impact. Feel free to work independently or in groups. Get creative, show off your skills and most importantly – have fun!

Entries will be accepted March 4 – April 4, 2016.

Finalist PSAs will be shown during the Information Security Forum, held on April 14-15, 2016. The winning PSAs will also be made available for Security Awareness Month.

If you have any questions regarding the PSA Challenge, contact ISF@dir.texas.gov.